ISSN 2312 9557. Вісник Дніпропетровського університету. Серія: Математика. 2016, вип. **21**

УДК 511.172

Н. В. Калашнікова

Дніпропетровський національний університет імені Олеся Гончара,
Дніпропетровськ 49050. *E-mail: natalja_nk@ukr.net*

Деякі властивості простих чисел спеціального вигляду та чисел Кармайкла

Досліджені деякі властивості будови мультиплікативної групи Z_m^* у випадку, коли m — просте число Мерсенна, Ферма або число Кармайкла. За допомогою цих висновків одержані властивості простих чисел Мерсенна і Ферма, а також чисел Кармайкла.

Ключові слова: число Мерсенна, число Ферма, число Кармайкла, конгруентність, мультиплікативна група.

Исследованы некоторые свойства строения мультипликативной группы Z_m^* в случае, когда m — простое число Мерсенна, Ферма или число Кармайкла. С помощью этих выводов получены свойства простых чисел Мерсенна и Ферма, а также чисел Кармайкла.

Ключевые слова: число Мерсенна, число Ферма, число Кармайкла, конгруентность, мультипликативная группа.

Some properties of structure of the multiplicative group Z_m^* are investigational, in the case, when m is Mersenne prime, Fermat or Carmichael number. With these findings obtsined properties of Mersenne primes and Fermat and Carmichael numbers.

Key words: Mersenne prime, Fermat prime, Carmichael number, congruence, multiplicative group.

Прості числа відіграють значну роль у криптографії. У зв'язку з тим, що багато криптографічних систем застосовують властивості простих чисел, розклад числа на прості множники, дослідження властивостей простих чисел стають ще важливішими. Під простими числами спеціального вигляду розуміють такі прості числа, які можна подати у визначеному алгебричному виді. Наприклад, числа Мерсенна і числа Ферма іноді бувають простими. Числом Мерсенна називають число, яке має вигляд $M_n = 2^n - 1$, де $n \in N$. Із означення випливає, що якщо число Мерсенна M_n просте, то n також просте. Число вигляду $F_n = 2^{2^n} + 1$, де $n \in N^0$, називають числом Ферма.

Твердження 1. Нехай $M_p = 2^p - 1$ — просте число Мерсенна. Тоді правдиві нижчеподані висловлювання:

1) для будь-якого натурального a, $2 \leq a \leq 2^p - 2$, і кожного натурального n число $a^{2^n} - 1$ не ділиться на M_p;

2) для деякого натурального a, $2 \leq a \leq 2^p - 3$, $(a^3 - 1) \vdots M_p$;

3) число $2^p + 1$ – складене;

4) якщо $p = 6k + 1$ $(k \in N)$, то група $Z^*_{M_p}$ має елементи порядку 7 і 9.

Доведення. 1) Оскільки число M_p просте, то $Z^*_{M_p}$ – циклічна група парного порядку, а отже, $Z^*_{M_p}$ має єдиний елемент порядку 2. Таким чином, серед натуральних чисел із проміжку $[1; 2^p - 1]$ конгруенція $a^2 \equiv 1(mod \quad M_p)$ є правильна тільки для 1 і $2^p - 2$.

$|Z^*_{M_p}| = 2^p - 2 = 2(2^{p-1} - 1)$. Оскільки число $2^{p-1} - 1$ непарне, то група $Z^*_{M_p}$ не має елементів порядку 2^n у разі $n \geq 2$, а отже, в проміжку $[1; 2^p - 1]$ є тільки два натуральні числа a такі, що $a^{2^n} \equiv 1(mod \quad M_p)$ — це 1 і $2^p - 2$;

2) оскільки число $p - 1$ парне, то $2^{p-1} - 1 \equiv 0(mod \quad 3)$, а отже, група $Z^*_{M_p}$ має елемент порядку 3. Звідси випливає, що $a^3 \equiv 1(mod \quad M_p)$ для деякого натурального a, $2 \leq a \leq 2^p - 3$;

3) оскільки число $2^p - 1$ просте, то $2^p - 1 = 6k + 1$ для деякого $k \in N$. Звідси випливає, що $2^p + 1 = (6k + 3)\vdots 3$;

4) $2^{6k+1} - 2 \equiv 64^k \cdot 2 - 2 \equiv 1^k \cdot 2 - 2 \equiv 0(mod \quad 63)$, а отже, $|Z^*_{M_p}|\vdots 63$.

Твердження 2. Нехай $F_k = 2^{2^k} + 1$ – просте число Ферма. Тоді слушні нижчеподані висловлювання:

1) для будь-якого натурального a, $2 \leq a \leq 2^{2^k} - 1$, число $a^2 - 1$ не ділиться на F_k;

2) якщо n — непарне натуральне число і $2 \leq a \leq 2^{2^k}$, то $a^n - 1$ не ділиться на F_k;

3) для будь-якого натурального m, $m \leq 2^k$ існують у точності 2^m натуральні числа a, менші за F_k і такі, що $a^{2^m} \equiv 1(mod \quad F_k)$;

4) для будь-якого непарного m правильна конгруенція

$$(3^m)^{\frac{F_k-1}{2}} \equiv -1(mod \quad F_k);$$

5) якщо $k \equiv 3(mod 4)$ і число Мерсенна M_k - просте, то $M_k{}^{\frac{F_k-1}{2}} \equiv -1(mod \quad F_k)$.

Доведення. 1) оскільки F_k — просте число, то $Z^*_{F_k}$ — циклічна група порядку 2^{2^k}. Таким чином, $Z^*_{F_k}$ має єдиний елемент порядку 2, а отже, серед натуральних чисел із $[1; 2^{2^k} + 1]$ конгруенція $a^2 \equiv 1(modF_k)$ є правильна тільки для 1 і 2^{2^k};

2) $|Z^*_{F_k}| = 2^{2^k}$, а отже, у групі $Z^*_{F_k}$ немає елементів непарного порядку;

3) циклічна група порядку 2^{2^k} для будь-якого $m \leq 2^k$ має точно одну підгрупу порядку 2^m;

4) $|Z^*_{F_k}| = 2^{2^k}$, таким чином, $ord_{F_k}3$ ділить 2^{2^k}. Оскільки

$$(\frac{3}{F_k}) = (\frac{F_k}{3}) \cdot (-1)^{\frac{F_k-1}{2}} \cdot \frac{3-1}{2} = (\frac{F_k}{3}) = (\frac{2}{3}) = -1,$$

то 3 є квадратичний нелишок за модулем F_k, а отже, $3^{\frac{F_k-1}{2}} \equiv -1(mod \quad F_k)$. З того, що $ord_{F_k}3$ є дільник числа 2^{2^k} і $3^{\frac{F_k-1}{2}} \equiv -1(mod \quad F_k)$ випливає, що $ord_{F_k}3 = 2^{2^k}$, тобто число 3 є первісний корінь за модулем F_k, і числа виду 3^m, де $(m, 2^{2^k}) = 1$, також є первісні корені за модулем F_k;

5) оскільки число M_k — просте, то k також просте, а отже, за малою теоремою Ферма $2^{2^k-1} \equiv 2(mod \quad 2^k - 1)$, таким чином,

$$F_k = 2^{2^k} + 1 = 2 \cdot 2^{2^k-1} + 1 \equiv 2 \cdot 2 + 1 \equiv 5(modM_k).$$

Далі маємо $M_k^{\frac{F_k-1}{2}} \equiv (\frac{M_k}{F_k}) \equiv (\frac{F_k}{M_k}) \equiv (\frac{5}{M_k}) \equiv (\frac{M_k}{5}) \equiv (\frac{2}{5}) \equiv -1(modF_k)$

. Основою ефективних тестів на простоту в криптографії є мала теорема Ферма: Якщо число n — просте і $(a, n) = 1$, то $a^{n-1} \equiv 1(mod \quad n)$.

Перевірку цієї умови називають тестом Ферма. Застосування тесту Ферма гарантує якісний результат тільки в одному разі, оскільки існують складені числа, які проходять це тестування, якщо a не є їх дільник. Складене число n, для якого за всіх натуральних чисел a, взаємно простих із n, правдива конгруенція $a^{n-1} \equiv 1(mod \quad n)$, називають числом Кармайкла. Із цього означення також можна одержати еквівалентне йому: складене число n є числом Кармайкла тоді й тільки тоді, коли за всіх натуральних чисел a правильна конгруенція $a^n \equiv a(mod \quad n)$.

Критерій Корселта. Непарне складене число n є число Кармайкла тоді й тільки тоді, коли для кожного його простого дільника p виконано дві умови:

1) число n не ділиться на p^2; 2) число $p - 1$ ділить $n - 1$.

Із критерію Корселта випливає, що в канонічному розкладі числа Кармайкла не менше трьох простих множників.

Твердження 3. Нехай $p_1, p_2, \ldots, p_m$ — множина простих чисел, модулі яких не перевищують фіксоване натуральне число M. Тоді існує лише скінченна множина простих чисел q таких, що $p_1p_2 \cdots p_mq$ є число Кармайкла.

Доведення. Припустимо, що $p_1p_2 \cdots p_mq$ — число Кармайкла. Із критерію Корселта випливає, що $p_1p_2 \cdots p_mq - 1$ ділиться на $q - 1$. Маємо

$$p_1p_2 \cdots p_mq - 1 = p_1p_2 \cdots p_mq - p_1p_2 \cdots p_m + p_1p_2 \cdots p_m - 1 = \\ = p_1p_2 \cdots p_m(q - 1) + p_1p_2 \cdots p_m - 1.$$

Звідси випливає, що вираз $p_1p_2 \cdots p_m - 1$ ділиться на $q - 1$. Але якщо $q > M^m$, то цю умову не буде виконано.

Твердження 4. Нехай n - число Кармайкла і $n = p_1p_2 \cdots p_m$, де $p_1, p_2, \ldots, p_m$ є різні прості числа. Тоді існує точно $2^m - 1$ чисел a, $2 \leq a \leq n - 1$, таких, що $a^2 \equiv 1(mod \quad n)$.

Доведення. Кількість елементів порядку 2 у групі Z_n^* дорівнює числу $2^m - 1$.

Твердження 5. Нехай n — число Кармайкла і $n = p_1p_2 \cdots p_m$, де $p_1, p_2, \ldots, p_m$ — різні прості числа, $p_i - 1 = 2^{s_i} \cdot t_i$ $(1 \leq i \leq m)$, де t_i — непарне число, $n - 1 = 2^s \cdot t$, де t — непарне число і M — найбільше з чисел $s_1, s_2, \ldots, s_m$. Тоді $M \leq S$.

Доведення. Група Z_n^* містить елементи порядків 2^{s_i} $(1 \leq i \leq m)$. Нехай $\bar{a}$ - елемент групи Z_n^* порядку 2^M. Якщо припустити, що $M > S$, то одержимо, що $a^{n-1} - 1$ не ділиться на n.

Библиографические ссылки

1. *Б*осс, В. Лекции по математике. Теория чисел [Текст] / В. Босс - М.: URSS. - 2013. Том 14.- 214 с.
2. *К*рэндалл, Р. Простые числа. Криптографические и вычислительные аспекты [Текст] / Р. Крэндалл, К. Померанс - М.: URSS. - 2011.- 663 с.

Надійшла до редколегії 15.02.2016